Newsbytes, 3/18

Raymond D. Aller, MD, and Hal Weiner

How hospitals use savvy and software as a phishing net

We all know we shouldn't click on suspicious emails, but suppose you see an email from your department of human resources with an attached document about a new dress code. You open it, thinking "*What* new dress code?" And now you've infected the hospital's computer system with a virus.

"The number of people who fell for that one was astounding," says Anahi Santiago, chief information security officer for Christiana Care, a two-hospital system headquartered in Wilmington, Del. Fortunately, it was just a drill—part of Christiana Care's ongoing campaign against phishing, or using fake email to trick recipients into abetting a cyberattack.

While the system's mail filters catch about 90 percent of malicious emails, Christiana Care's approximately 12,000 email users are the last line of defense for those that sneak through, and Santiago tests them quarterly with simulated attacks created by Wombat Security Technologies. If employees click something they shouldn't, they have to take anti-phishing refresher training, she explains. The software immediately sends them a "teachable moment" message offering tips to avoid future traps and schedules them for a more detailed five- to 15-minute interactive course. While Santiago did not provide specific figures, she says using the testing program has reduced employee failure rates "exponentially."

"We use six different templates that are sent randomly to our users to lower the likelihood that employees who work in a particular department will get the same test email," Santiago says. "However, if they were to share that it's a test, we would not be concerned—at least they would be talking about it, which in turn generates awareness."

A skilled phishing attack can look like a genuine internal message, complete with corporate logo, says Wombat spokeswoman Amy Baker. Some messages even appear to be from a specific sender, such as an organization's chief financial officer, a tactic known as spear-phishing. Many organizations' email formats are standardized and easy to guess. A hacker can deduce a top executive's email address and include it as part of the message, even though the true originating address is outside the organization, and maybe even outside the country.

HHS's Office for Civil Rights, which investigates breaches of protected health information, reported 42 incidents, over the past two years, of hackers attacking health care providers via email. Each incident breached the information of between 500 and 80,000 people. (Incidents affecting fewer than 500 people are not reported to the OCR.) Email attacks on providers represent about one in 10 data breaches reported to the OCR since 2016.

Health care employees are less likely than those in other industries to recognize a phishing email if they haven't had anti-phishing training, according to Wombat's 2017 "State of Security Education—Healthcare" study. On average, they missed 31 percent of questions in a training module on how to identify a phishing threat, compared with 28 percent of employees across all industries. Yet the company's 2018 "State of the Phish" report indicates that they are less likely to open phishing messages. Only 10 percent of health care employees in the latter study clicked on a simulated phishing email, a better record than either government (13 percent) or tech (12 percent). Defense contractors did the best, at three percent.

Hackers would rather filch passwords from unwary users or get them to click on a malicious link before they try a direct assault on a computer, says Ryan Hardesty, founder of PhishingBox, also a provider of phishing simulation software for employee training. Documents such as health records command a premium on the dark Web, he notes. A fake note from a CFO, instructing the recipient to pay the attached vendor's invoice with a wire transfer, can yield an immediate cash bonanza. Phishing is also a way to install ransomware to freeze a hospital's computer system.

In response to the uptick in cybercrimes, many health care organizations are hardening their defenses against phishing. Kaleida Health, an 11-hospital system in Buffalo, NY, recently banded together with its regional competitors in a coordinated anti-phishing campaign after Kaleida suffered a phishing attack last summer that compromised information on almost 3,000 patients. “We realized that a lot of our providers move between organizations and we all needed to be on the same page with our policies,” says Cletis Earle, Kaleida’s chief information officer. All the health care system CIOs and chief information security officers consult with one another and trade ideas with Buffalo area banks and educational institutions, also frequent phishing targets.

East Alabama Medical Center, Opelika, Ala., uses PhishingBox’s software to run monthly anti-phishing contests. The IT security staff picks 10 to 20 departments and sneaks phishing messages into their daily emails. At the end of the month, the targeted departments are ranked according to how many of their employees succumbed to one or more of the messages. IT security administrator Michael Wegner is proud to say that the average failure rate is one to two percent, and enough departments score 100 percent success that it’s impractical to offer a trophy to the winner. Wegner has also trained people to forward suspicious email to his department.

“Our platform is structured so that employees can easily report suspicious emails to the designated individuals,” explains PhishingBox’s Hardesty. And PhishingBox, like Wombat, offers multiple-template campaigns to organizations concerned about employees sharing their phishing experiences.

“Now and then,” says Wegner, “someone will send us a real phishing email and say, ‘Ha, you didn’t get me this time!’ And we say, ‘That wasn’t one of ours.’”

Teaching employees to flag a potential threat isn’t always easy, however, since people are often distracted or hurrying through email messages. It takes a conscious effort to hover before you click, for example. By hovering over an email address or a link, you can often see where it really came from or where it will go. If the information you get from hovering doesn’t match that in the original message, you’re being phished, says Earle.

Employees should also watch for external mail pretending to be internal mail, the experts say. Some mail servers tag outside mail with [EXTERNAL] or something similar in the subject line. Some don’t show addresses for internal senders, just names. A phishing attempt typically will look like an external message, even if it claims to be internal.

Phishing messages have better spelling and grammar than they used to, but if the language sounds off, or if it’s asking you to do something that’s not normal procedure, send it to your IT security team for verification, says Earle. “If it smells phishy, it is.”*—Elizabeth Gardner*
[hr]

Netlims releases report and mobile app

Netlims recently posted on its website a white paper, titled “The Path to More Revenue: Cloud-Based LIMS, Mobile Apps, and Point-of-Care Telehealth,” and introduced a mobile app for phlebotomy and other point-of-care uses.

The white paper details how Netlims products can enhance patient outcomes, contribute to client revenue, and foster compliance with Medicare quality-based payment programs. It specifically addresses the benefits of the company’s LabOS lab information system and new LabWay patient-centric mobile app.

LabWay can be integrated with LabOS and POC diagnostic devices from mobile telehealth technology companies such as RPM Telehealth and V-Patch. It provides mobile phlebotomists with the information necessary to perform collections, manage shipments, plan and save travel routes, and address other aspects of off-site visits.

Netlims*, 908-566-7700*

[hr]

Inspirata purchases Omnyx

The digital pathology workflow solutions and cancer informatics provider Inspirata has acquired Omnyx from GE Healthcare.
Omnyx's flagship digital pathology software product, Dynamyx, connects pathologists and other care providers to foster collaboration in cancer care and improve cancer diagnostics.

"The acquisition of Omnyx positions Inspirata with the most comprehensive digital pathology workflow solution in the world," said Inspirata CEO Satish Sanan, in a press release. "It brings us the last mile to reach our goal of having an end-to-end integrated pathology solution with a scanner-agnostic whole slide image viewer and image-management system. It also gives us a fully supported IVD device cleared for primary digital diagnosis in Europe and Canada, and it expands our customer base and geographic footprint across those countries."

Inspirata plans to retain Omnyx's employees and use the company's Pittsburgh office as a center of excellence for digital pathology software development. "Our short-term plan," added Sanan, "is to rapidly combine the advantages of our digital pathology software platform and the Dynamyx platform by converging them onto a shared, state-of-the-art technology stack."

***Inspirata**, 813-570-8900*

[hr]

KLAS Enterprises announces annual vendor honors

For the eighth consecutive year, Epic has received a top honor in KLAS Enterprises' annual Best in KLAS awards, earning the ranking of number one overall software suite for its EpicCare inpatient electronic medical record system. The company received numerous recognitions in the 2018 ranking, including Best in KLAS in the laboratory (large hospital/IDN) category for its Epic Beaker lab system.

The "2018 Best in KLAS: Software & Services" report names the top-performing health care information technology companies within various market segments based on feedback from health care providers.

Also receiving more than one honor from the health information technology market research firm were Cerner, a repeat category leader in anatomic pathology for its CoPathPlus system; Meditech, once again the recipient of the Best in KLAS designation for community hospital information system, for its Meditech C/S and 6x; and Optimum Healthcare IT, ranked top overall IT services firm for the second year in a row. Orchard Software too retains its position as category leader in laboratory (community hospital/ambulatory) for its Orchard Harvest LIS.

A list of the 2018 Best in KLAS awardees is available at www.klas
research.com/best-in-klas-winners.
[hr]

Dr. Aller teaches informatics in the Department of Pathology, University of Southern California, Los Angeles. He can be reached at raller@usc.edu. Hal Weiner is president of Weiner Consulting Services LLC, Eugene, Ore. He can be reached at hal@weinerconsulting.com.